SEALED

U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED
FEB - 3 2016
CLERK, U.S. DISTRICT COURT
By _____ Deputy

United States District Court

NORTHERN DISTRICT OF TEXAS

In the Matter of the Search of
(Name, address or Brief description of person, property or premises to be searched)

ALL RECORDS OF SMARSH, 851 SW 6TH AVENUE, SUITE 800, PORTLAND, OREGON 97204, ASSOCIATED WITH THE CUSTOMER OR SUBSCRIBER "NOVUS HEALTH SERVICES, INC."

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 3:16-MJ- 69- BH

I Thomas R. Cook **being duly sworn depose and say:**
I am a(n) Special Agent with the Federal Bureau of Investigation (FBI) and have reason to believe that on the person of or XX on the property or premises known as (name, description and/or location)

(SEE ATTACHMENT A).

in the NORTHERN District of TEXAS there is now concealed a certain person or property, namely (describe the person or property to be seized)

(SEE ATTACHMENT B).

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)
property that constitutes evidence of the commission of a crime, contraband, the fruits of crime, and is, otherwise, criminally possessed, **concerning a violation of Title** 18 **United States code, Section(s)** 1035, 1343, 1349, 1347 and 1518. **The facts to support a finding of Probable Cause are as follows:**

(SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT THOMAS R. COOK).
Continued on the attached sheet and made a part hereof. XX **Yes** __ **No**

Signature of Affiant
THOMAS R. COOK
Special Agent, FBI

Sworn to before me, and subscribed in my presence

February 3, 2016 **at** **Dallas, Texas**
Date and Time **City and State**

IRMA C. RAMIREZ
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

ATTACHMENT A
Property to Be Searched

This warrant applies to all records, data, and information associated with the customer or subscriber Novus Health Services, Inc., that is stored at premises owned, maintained, controlled, or operated by Smarsh, a company headquartered at 851 SW 6th Avenue, Suite 800, Portland, Oregon 97204.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Smarsh.

To the extent that the information described in Attachment A is within the possession, custody, or control of Smarsh, including any messages (including archived messages), records, passwords files, logs, or information that have been deleted but are still available to Smarsh or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Smarsh is required to disclose the following information to the government:

a. All records or other information pertaining to Novus Health Services, Inc. (Novus), including all files, passwords, databases, and database records stored by Smarsh in relation to Novus. This includes copies of any DVDs or other digital storage media containing archived information, including emails, that were sent from Smarsh to Novus or any of Novus's representatives as part of the services Smarsh has provided to Novus, and any passwords necessary to access those DVDs or other digital storage media.

b. All records, including logs recording any access (or attempted access) to any account held by Novus or anyone representing or purporting to represent Novus, or any modification (or attempted modification) of the contents any such account.

c. All communications, including emails, to or from anyone representing or purporting to represent Novus regarding any Smarsh account held by Novus or anyone representing or purporting to represent Novus.

d. All data, including emails and other communications, collected in the course of any archiving service that Smarsh provided to Novus or anyone representing or purporting to represent Novus.

e. All information associated with any Smarsh account held by Novus or anyone representing or purporting to represent Novus. For each such account, the information should include:

- The account holder's name and address.
- Any account number or other account-identifying information.
- The address of any website where the account can be accessed.
- Any userid or other login information, and any passwords associated with the account.
- The length of service for each account, including start date, and types of service utilized.
- Means and source of payment for each service (including any credit card or bank account number).
- All account history.

f. All user connection and transaction logs associated with each and every account identified in paragraph (e), above, including all available IP logs, connection time and date, disconnect time and date, method of connection to system, and data transfer volume.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1035 (False Statements relating to Health Care Matters); 18 U.S.C. § 1343 (Fraud by Wire); 18 U.S.C. § 1349 (Conspiracy to Commit Health Care Fraud); 18 U.S.C. § 1347 (Health Care Fraud); and 18 U.S.C. § 1518 (Obstruction of criminal investigation of health care offenses), including but not limited to:

a. All passwords necessary to access any relevant information (as described in the preceding paragraph) archived by Smarsh for Novus, in particular sixty-two DVDs provided to Novus by Smarsh, eighteen of which were obtained by the FBI during a warrant executed at Novus's place of business on September 17, 2015, and forty-four of which were obtained via grand jury subpoena on November 30, 2015.

b. All records, communications, or data that relate to the provision of home health or hospice medical care services to patients. Such records, communications, or data would include but not be limited to those that relate to patient certification for either home health or hospice care, patient plans of care, the medication of any patient under

home health or hospice care, and the length of stay of any patient under home health or hospice care.

c. All records, communications, or data that relate to the control and operation of Novus, the CMS aggregator cap, the billing of Medicare or Medicaid, and payments made to Medicare or Medicaid.

d. All user connection and transaction logs associated with any Smarsh account for which information has been provided, and that are relevant to the provision of home health or hospice medical care services to patients, the control and operation of Novus, the CMS aggregator cap, the billing of Medicare or Medicaid, and payments made to Medicare or Medicaid.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF ALL RECORDS OF SMARSH, 851 SW 6TH AVENUE, SUITE 800, PORTLAND, OREGON 97204, ASSOCIATED WITH THE CUSTOMER OR SUBSCRIBER "NOVUS HEALTH SERVICES, INC."	CASE NO. 3:15-MJ- **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Thomas R. Cook, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), currently assigned to the Dallas Division, duly appointed and acting according to law. I have been a Special Agent since August 2014. Prior to becoming a Special Agent, I worked for two and a half years as an Intelligence Analyst for the FBI on counterterrorism investigations. I am currently assigned to the Criminal Branch of the Dallas Division and am responsible for conducting investigations of health care fraud, to include fraud against government programs such as Medicare and Medicaid. I have received training in such areas as electronic and physical surveillance, interviewing witnesses and defendants, financial analysis, collection of evidence, and the use of confidential informants. I have also received training regarding computers and digital evidence.

2. This affidavit is made in support of an application pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and 2703(g), and Federal Rule of Criminal Procedure 41, for a warrant to search the records of Smarsh, 851 SW 6th Avenue, Suite 800, Portland, Oregon 97204, associated with the customer or subscriber Novus Health Services, Inc. (Novus) and as more fully described in Attachment A, for the evidence, fruits, and instrumentalities of crimes specified in Attachment B.

3. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that Brad Harris (Harris), Amy Nafziger-Harris (Nafziger-Harris), and other co-conspirators have committed federal crimes including Health Care Fraud in violation of 18 U.S.C. § 1035 (False Statements relating to Health Care Matters); 18 U.S.C. § 1343 (Fraud by Wire); 18 U.S.C. § 1349 (Conspiracy to Commit Health Care Fraud); 18 U.S.C. § 1347 (Health Care Fraud); and 18 U.S.C. § 1518 (Obstruction of criminal investigation of health care offenses); and that evidence, fruits and instrumentalities of these crimes, as further described in Attachment B, will be found in the records of Smarsh associated with the customer Novus. Pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), this application seeks to compel Smarsh, a remote computing service, to disclose to the government all records and other information in its possession pertaining to the customer Novus, to be searched for the records, data, and information specifically described in Attachment B.

4. The facts in this affidavit come from my personal observations, my review of the investigative materials compiled in this case, my training and experience, and information obtained from other agents, including Special Agent Jeffery Ford of the

United States Department of Health and Human Services Office of Inspector General (HHS-OIG). This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")

5. The Stored Communications Section of the Electronic Communications Privacy Act (ECPA), codified at 18 U.S.C. §§ 2701-2712, and as amended, defines the legal process a government entity must obtain to gain access to specified records of a customer or subscriber of a computer network service provider. Section 2703 provides, in pertinent part:

> **(a) Contents of wire or electronic communications in electronic storage.** – A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.
>
> **(b) Contents of wire or electronic communications in a remote computing service.** – (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection,
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure

(or in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; . . . .

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service-

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service. – (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity-

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; . . . .

6. As used in 18 U.S.C. § 2703:

a. The term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system. *See* 18 U.S.C. § 2711(2);

b. The term "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. *See* 18 U.S.C. § 2510(8);

c. The term "electronic communications system" means any wire, radio electromagnetic, photo optical or photo electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. *See* 18 U.S.C. § 2510(14);

d. The term "electronic communications service" means any service which provides to users thereof the ability to send or receive wire or electronic communications. *See* 18 U.S.C. § 2510(15); and,

e. The term "electronic storage" means any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication. *See* 18 U.S.C. § 2510(17).

7. The pertinent provisions of § 2703 quoted above authorize a court with jurisdiction over the underlying offense to issue a search warrant for records of an electronic communications service or remote computing service nationwide. Thus, if jurisdiction over the offense described in this affidavit lies in the Northern District of

Texas, this Court is authorized to issue the instant search warrant to obtain records held by Smarsh.

FACTS ESTABLISHING PROBABLE CAUSE

6. Based on my training and experience and the facts set forth in this affidavit there is probable cause to believe that Brad Harris (Harris), Amy Nafziger-Harris (Nafziger-Harris), and other co-conspirators have committed federal crimes including Health Care Fraud in violation of 18 U.S.C. § 1035 (False Statements relating to Health Care Matters); 18 U.S.C. § 1343 (Fraud by Wire); 18 U.S.C. § 1349 (Conspiracy to Commit Health Care Fraud); 18 U.S.C. § 1347 (Health Care Fraud); and 18 U.S.C. § 1518 (Obstruction of criminal investigation of health care offenses), and that evidence thereof can be found in the materials described in Attachment B.

7. The Medicare Program ("Medicare") is a federal health care benefit program providing benefits to persons who are over the age of sixty-five or disabled. Medicare is administered by the United States Department of Health and Human Services (HHS) through its agency, the Centers for Medicare & Medicaid Services (CMS). Medicare will help pay for inpatient hospital stays, skilled nursing facility services, home health care, and hospice care provided by qualified providers. The Medicaid program is a state-administered health insurance program funded predominantly by the United States Government and administered in Texas by the State of Texas. The Medicaid program helps pay for reasonable and necessary medical procedures and services provided to individuals who are deemed eligible under state low-income programs.

8. For healthcare providers who provide care under Medicare and Medicaid, hospice care provides greater opportunities for revenue than home health care. However, hospice providers are subject to an "aggregator cap," which is calculated at the end of each calendar year by CMS based on the average cost of a Medicare patient hospice stay. A provider who has received Medicare reimbursements for hospice patient services will be required to pay back to Medicare amounts paid for services that exceed the calculated cap amount. Hence, hospice providers have an incentive to enroll patients whose hospice stays will be short relative to the cap. Even under Medicaid, extended hospice care will result in regulatory scrutiny, which would be unwanted if the decision to administer hospice care was unmerited. For understandable reasons, the decision to move a patient from home health (i.e., remedial) care to hospice (i.e., palliative) care can only be made by a licensed medical professional (i.e., a doctor), who must sign a certification form as required by Medicare and Medicaid guidelines.

9. The FBI, HHS-OIG, and the Medicaid Fraud Control Unit (MFCU) have jointly been investigating the activities of Novus and its CEO, Harris, since on or about October 17, 2014. The investigation initially focused on allegations that starting on or about January 1, 2012, Novus's management recruited patients for their home health and hospice business that did not qualify for services and charged Medicare and Medicaid for services that were not medically necessary. Investigators learned throughout the course of their investigation that, as part of this scheme, Harris, who has no medical training or licenses, would direct his employed nurses to overdose hospice patients with palliative medications such as morphine to hasten death, and thereby minimize Novus's payback

obligations under the CMS aggregator cap. These allegations became the focus of the investigation.

10. Evidence gathered in this investigation reveals that Harris was trying to manipulate the aggregator cap by directing patients to be moved to or from home health and hospice service without regard to their actual medical needs. CW-1, a nurse employed by Novus, told Special Agent Ford that Harris would routinely decide which home health patients would be moved to hospice. He did this by having employees who were not doctors sign the certifications with the names of doctors also employed by Novus, without ever having the doctors examine the patients. If a patient was on hospice for too long, Harris would direct the patient be moved back to home health, irrespective of whether the patient needed continued hospice care. CW-1 also told Special Agent Ford that Harris would typically issue these instructions via text message. Harris's purpose was to continue receiving Medicare and Medicaid reimbursements without exceeding the CMS aggregate cap or inviting scrutiny of hospice practices.

11. Information provided by a second Novus employee, CW-2, indicates that Harris also directed the falsification of records documenting what services were provided to patients under Novus's care. CW-2, who described him/herself as Harris's friend and assistant, explained to investigators that his/her responsibilities at Novus included entering patient data into company computers for the purpose of processing Medicare claims. On multiple occasions, CW-2 reported that he/she received patient treatment consent forms, necessary for Novus to file a Medicare or Medicaid claim, that were unsigned by the patients who supposedly received the treatment. When CW-2 brought

the unsigned forms to Harris's attention, Harris would tell him/her to have Harris's wife, Nafziger-Harris, sign for the patient. CW-2 would then take the forms to Nafziger-Harris, who would sign them in the patients' names. CW-2 would then process the consent forms for use in Medicare reimbursement applications.

12. CW-2 explained that on multiple occasions Harris expressed concern that Novus was losing money on its Medicare reimbursements because long-living patients were causing Novus to exceed the CMS aggregator cap. CW-2 gave several examples of this behavior. During a lunch conversation with two "marketers" – individuals hired to inform doctors of Novus's availability for home health and hospice services – Harris asked the marketers to "find patients who would die within twenty-four hours" because that would "save my ass toward the cap." During another lunchtime conversation, Harris, speaking of a Novus hospice patient, said words to the effect of, "if this fucker would just die." CW-2 understood Harris to mean that he wished the patient would die so as to bring down the average stay of patients at Novus in order to come under the CMS aggregator cap.

13. Other employees investigators have spoken with, specifically nurses employed by Novus, confirmed that Harris was concerned about the CMS aggregator cap limiting Medicare reimbursements and wanted to reduce Novus's patient-stay average by enrolling hospice patients who would die quickly.

14. On September 2, 2015, investigators met with CW-4, a nurse case manager for both Novus's hospice and home health businesses. CW-4 stated that Harris had requested via text message that he/she administer an overdose of medication to a hospice

patient on or about October 17, 2013 by increasing the patient's medication dosage to approximately four times the maximum allowed. CW-4 told Harris that he/she would comply with his request, but did not do so because he/she knew that it would kill the patient.

15. On September 14, 2015, CW-5, who is a registered nurse and employed by Novus as a hospice patient case manager, told Special Agent Ford during a telephone conversation that Harris regularly directs nurses, generally via text message or other electronic communication, to overdose hospice patients when they have been on hospice service for too long, and that Harris directed him/her to overdose three patients, two of whom he/she could identify by name; the third he/she could not recall. CW-5 said that the request to overdose all three patients was sent to him/her about eight months ago via a text message from Harris, which he/she received on a phone that was issued to him/her by Novus.

16. CW-5 said that the nurses at Novus call Harris "Dr. Brad" because he often directs them, generally via text message or other electronic communication, to give medication to patients with specific dosage amounts, even though he has no medical training. CW-5 also stated that Harris directs nurses to overdose hospice patients, often by text message, and uses expressions like "you need to make this patient go bye-bye." CW-5 said that it was commonly understood among the nurses that Harris gave instructions to overdose patients in order to kill them, and thereby reduce the average patient stay so that it fell below the CMS aggregator cap limiting Medicare reimbursements.

17. As part of its business practices, Novus had its company-wide email system backed up by Smarsh. Smarsh would routinely send Novus DVDs which contained copies of emails archived from Novus's online email system. In order to access the DVDs, an authorized employee of Novus would have to contact Smarsh, which would provide a password to grant access. The FBI currently has lawful possession of sixty-two of the DVDs provided to Novus by Smarsh (the "Smarsh DVDs"). The Smarsh DVDs are currently located at the FBI, One Justice Way, Dallas, Texas 75220. Investigators obtained eighteen Smarsh DVDs during a search warrant executed at Novus's place of business on September 17, 2015. The remaining forty-four were obtained via grand jury subpoena on November 30, 2015, from CW-6's attorney. CW-6 is a former high-ranking employee of Novus.

18. On February 22, 2015, the government obtained a search warrant to search the Smarsh DVDs, but investigators could not access them because agents did not have the necessary passwords.

19. Given these facts and the inferences from these facts, I submit there is probable cause to believe that the information described in Attachment B is necessary to access the Smarsh DVDs, and is potentially relevant to the current investigation into Harris, Nafziger-Harris, and the other Novus co-conspirators described above. With this warrant application, the government also seeks to have Smarsh disclose any additional data, including emails, that it has archived as a remote computing service for Novus, and which investigators have not yet obtained through other sources.

SEARCH AND SEIZURE OF DIGITAL EVIDENCE

20. This Court has jurisdiction to issue the requested warrant because it is a "court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, this Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

21. I anticipate executing this proposed warrant under the Electronic Communications Privacy Act. *See* 18 U.S.C. §§ 2701 – 11. Under this Act, the presence of a law enforcement officer is not required for the service or execution of this proposed warrant. *See id.* § 2703(g). The Act, and in particular sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), authorize the Court to issue a warrant requiring Smarsh to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

For the reasons set forth above, I respectfully request that the Court issue a warrant authorizing a search of all records of Smarsh associated with the customer or subscriber "Novus Health Services, Inc.," as further described in Attachment A, and the seizure of any such records that are evidence, fruits, or instrumentalities of the federal offenses identified above, set out in detail in Attachment B.

Respectfully submitted,

Thomas R. Cook
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 3rd day of February 2016.

HONORABLE IRMA C. RAMIREZ
UNITED STATES MAGISTRATE JUDGE